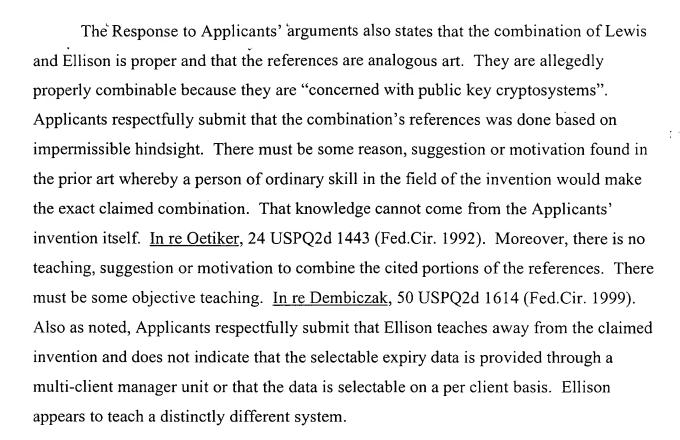private signing key expiry data that are selectable on a per client basis when the digital signature key pairs are not shared among users. Accordingly, the claim requires providing selectable expiry data, through a multi-client manager unit, not through a client unit a alleged in the Office Actions. Accordingly, Applicants' assertion is respectfully correct.

In addition, in response to Applicants' arguments, the response states "there is no multi-client trust authority reciting in claims, nor can this entity be found in the Specification, referring to "the sixth line of the second full paragraph on page 2 of Applicants' response." Applicants' attorney respectfully requests clarification. The second full paragraph on page 2, line 6 thereof does not contain the words "multi-client trust authority." Applicants believe that the Examiner meant to cite line 5 of the second full paragraph which is still not a correct characterization of Applicants' claims. Line 5 of paragraph 2 of Applicants' response specifically says that the Applicants claim, inter alia, providing "through a multi-client manager unit, selectable digital expiry data including ....". This is the exact claim language from Claim 1, for example. Accordingly, since the Examiner's characterization of the claims and the characterization of Applicants' argument is based on an apparent misunderstanding of the claim language. Applicants respectfully request allowance of the claims.

For argument's sake, even if the claim did claim "multi-client trust authority," Applicants respectfully submit that such a term is identical to "multi-client manager unit" since Applicants state, in the Specification on page 4, ll. 15-17 that the multi-client manager 12 is otherwise known as "a certification authority" that manages a number of clients. A certification authority is a well known term, (however, a certification authority that performs the operations described in Applicants' invention is quite unique). Accordingly, Applicants respectfully submit that the claims are in condition for allowance.

2

The Response to Applicants' arguments also states that the combination of Lewis and Ellison is proper and that the references are analogous art. They are allegedly properly combinable because they are "concerned with public key cryptosystems". Applicants respectfully submit that the combination's references was done based on impermissible hindsight. There must be some reason, suggestion or motivation found in the prior art whereby a person of ordinary skill in the field of the invention would make the exact claimed combination. That knowledge cannot come from the Applicants' invention itself. In re Oetiker, 24 USPQ2d 1443 (Fed.Cir. 1992). Moreover, there is no teaching, suggestion or motivation to combine the cited portions of the references. There must be some objective teaching. In re Dembiczak, 50 USPQ2d 1614 (Fed.Cir. 1999). Also as noted, Applicants respectfully submit that Ellison teaches away from the claimed invention and does not indicate that the selectable expiry data is provided through a multi-client manager unit or that the data is selectable on a per client basis. Ellison appears to teach a distinctly different system.

The final rejection again rejects Claim 1 arguing that the claims are obvious since it would have "been obvious to a person of ordinary skill in the art at the time the invention was made to give users the ability to define the validity period for certificates, as taught by Ellison in the public key update system of Lewis." Applicants again note that Applicants are not claiming that the users define the validity period. Applicants respectfully request a showing of the claim language that is thought to require this. An opposite approach is claimed. A multi-client managing unit (certification authority, for example) provides, inter alia, selectable digital signature expiry data including at least public verification key expiry data, and selectable private signing key expiry data, that are selectable on a per client basis wherein a digital signature key pairs are not shared among users. As such, a certification authority, or other trusted authority, has the ability to selectably vary public key verification expiry data and private signing key expiry data on a per client basis. Applicants are not claiming that a user provides defined validity

periods for their own certificates as apparently alleged in the Office Action. Applicants claim a distinctly different system.

Applicants also respectfully reassert the remarks made in the previous responses to the previous Office Actions.

Accordingly, Applicants respectfully submit that the claims are in condition for allowance. The Examiner is invited to contact the undersigned attorney by telephone or facsimile if the Examiner believes that such a communication would advance the prosecution of the present patent application.

Respectfully submitted,

MARKISON & RECKAMP, P.C.

By

Christopher J. Reckamp
Registration No 34,414

Date: February 1, 2001

MARKISON & RECKAMP, P.C.
P.O. Box 06229, Wacker Drive
Chicago, IL 60606-0229
(312) 939-9800
FAX: (312) 939-9828